

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

| | |
|---|-----------------------------|
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. WE INFORM, LLC, et al., Defendants. | Civ. Action No. 24-04037-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. INFOMATICS, LLC, et al., Defendants. | Civ. Action No. 24-04041-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THE PEOPLE SEARCHERS, LLC, et al., Defendants. | Civ. Action No. 24-04045-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DM GROUP, INC., et al., Defendants. | Civ. Action No. 24-04075-HB |

| | |
|---|-----------------------------|
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p style="text-align: center;">Plaintiffs,</p> <p>v.</p> <p>DELUXE CORPORATION, et al.,</p> <p style="text-align: center;">Defendants.</p> | Civ. Action No. 24-04080-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p style="text-align: center;">Plaintiffs,</p> <p>v.</p> <p>QUANTARIUM ALLIANCE, LLC, et al.,</p> <p style="text-align: center;">Defendants.</p> | Civ. Action No. 24-04098-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p style="text-align: center;">Plaintiffs,</p> <p>v.</p> <p>YARDI SYSTEMS, INC., et al.,</p> <p style="text-align: center;">Defendants.</p> | Civ. Action No. 24-04103-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p style="text-align: center;">Plaintiffs,</p> <p>v.</p> <p>DIGITAL SAFETY PRODUCTS, LLC, et al.,</p> <p style="text-align: center;">Defendants.</p> | Civ. Action No. 24-04141-HB |

| | |
|---|-----------------------------|
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. CIVIL DATA RESEARCH, et al., Defendants. | Civ. Action No. 24-04143-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SCALABLE COMMERCE, LLC, et al., Defendants. | Civ. Action No. 24-04160-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LABELS & LISTS, INC., et al., Defendants. | Civ. Action No. 24-04174-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. INNOVIS DATA SOLUTIONS INC., et al., Defendants. | Civ. Action No. 24-04176-HB |

| | |
|---|-----------------------------|
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ACCURATE APPEND, INC., et al., Defendants. | Civ. Action No. 24-04178-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. ZILLOW, INC., et al., Defendants. | Civ. Action No. 24-04256-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. EQUIMINE, INC., et al., Defendants. | Civ. Action No. 24-04261-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. MELISSA DATA CORP., et al., Defendants. | Civ. Action No. 24-04292-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. RESTORATION OF AMERICA, et al., Defendants. | Civ. Action No. 24-04324-HB |

| | |
|---|-----------------------------|
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>I360, LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04345-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>GOHUNT, LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04380-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>ACCUZIP, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04383-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>SYNAPTIX TECHNOLOGY, LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04385-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>JOY ROCKWELL ENTERPRISES, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04389-HB |

| | |
|---|-----------------------------|
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>E-MERGES.COM, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04434-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>NUWBER, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04609-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>ROCKETREACH LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04664-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>BELLES CAMP COMMUNICATIONS, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-04949-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>PROPERTYRADAR, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-05600-HB |

| | |
|--|-----------------------------|
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>THE ALESCO GROUP, LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-05656-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>SEARCHBUG, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-05658-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>AMERILIST, INC., et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-05775-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>US DATA CORPORATION, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-07324-HB |
| <p>ATLAS DATA PRIVACY CORPORATION, et al.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>SMARTY, LLC, et al.,</p> <p>Defendants.</p> | Civ. Action No. 24-08075-HB |

| | |
|--|-----------------------------|
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. COMPACT INFORMATION SYSTEMS, LLC, et al., Defendants. | Civ. Action No. 24-08451-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DARKOWL, et al., Defendants. | Civ. Action No. 24-10600-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. THOMSON REUTERS CORPORATION, et al., Defendants. | Civ. Action No. 24-04269-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. DELVEPOINT LLC, et al., Defendants. | Civ. Action No. 24-04096-HB |

| | |
|--|-----------------------------|
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. SPY DIALER, INC., et al., Defendants. | Civ. Action No. 24-11023-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. PEOPLEWHIZ, INC., et al., Defendants. | Civ. Action No. 25-00237-HB |
| ATLAS DATA PRIVACY CORPORATION, et al., Plaintiffs, v. LIGHTHOUSE LIST COMPANY, LLC, et al., Defendants. | Civ. Action No. 24-11443-HB |

**PLAINTIFFS' BRIEF IN OPPOSITION TO DEFENDANTS'
CONSOLIDATED MOTION TO DISMISS PURSUANT TO RULE 12(b)(6)**

Attorneys for Plaintiffs

PEM LAW LLP

Rajiv D. Parikh
Kathleen Barnett Einhorn
Jessica A. Merejo
One Boland Drive, Suite 101
West Orange, New Jersey 07052
Telephone (973) 577-5500
Email: rparikh@pemlawfirm.com
keinhorn@pemlawfirm.com
jmerejo@pemlawfirm.com

**BIRD MARELLA RHOW
LINCENBERG DROOKS NESSIM
LLP**

Ekwan E. Rhow (admitted *pro hac vice*)
Elliot C. Harvey Schatmeier (admitted
pro hac vice)
Bill L. Clawges (admitted *pro hac vice*)
1875 Century Park East, 23rd Fl
Los Angeles, California 90067
Telephone: (310) 201-2100
Email: erhow@birdmarella.com
ehs@birdmarella.com
bclawges@birdmarella.com

BOIES SCHILLER FLEXNER LLP

Adam Shaw (admitted *pro hac vice*)
30 South Pearl Street, 12th Floor
Albany, New York 12207
Telephone: (518) 434-0600
Email: ashaw@bsflfp.com

Mark C. Mao (admitted *pro hac vice*)
Julia Bront (admitted *pro hac vice*)
44 Montgomery Street, 41st Floor
San Francisco, California 94104
Telephone: (415) 293-6800
Email: mmao@bsflfp.com
jbront@bsflfp.com

James Lee (admitted *pro hac vice*)
Eric Palmer (admitted *pro hac vice*)
100 SE Second Street, Suite
2800 Miami, Florida 33131
Telephone: (305) 357-8434
Email: jlee@bsflfp.com
epalmer@bsflfp.com

MORGAN & MORGAN, P.A.

Ryan J. McGee (admitted *pro hac vice*)
John A. Yanchunis (admitted *pro hac vice*)
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Email: rmcgee@forthepeople.com
jyanchunis@forthepeople.com

TABLE OF CONTENTS

| | Page |
|--|-------------|
| TABLE OF AUTHORITIES | iii |
| PRELIMINARY STATEMENT | 1 |
| FACTUAL BACKGROUND..... | 3 |
| A. Daniel’s Law. | 3 |
| B. Defendants Violated Daniel’s Law By Failing to Timely Comply with the Nondisclosure Requests. | 4 |
| ARGUMENT | 5 |
| I. DEFENDANTS’ LIABILITY UNDER DANIEL’S LAW IS SUFFICIENTLY PLEADED. | 5 |
| A. The Complaints Plausibly Plead Facts Related to Assignments..... | 9 |
| B. The Complaints Plausibly Allege that the Individual Plaintiffs and Covered Persons Sent Their Own Notices..... | 11 |
| C. The Complaints Plausibly Allege Facts Establishing that the Nondisclosure Requests were Legally Sufficient. | 12 |
| D. The Complaints Plausibly Allege Facts Establishing that Defendants Received the Written Notices Sent to Them. | 14 |
| E. Plaintiffs Plausibly Allege that Defendants Possessed and Disclosed Protected Information..... | 16 |
| F. The Complaints Plausibly Allege Defendants’ Culpability..... | 17 |
| G. Plaintiffs’ Allegations Plausibly Establish Causation..... | 19 |
| H. Plaintiffs Have Alleged Damages. | 21 |
| I. The Court Should Not Strike Plaintiffs’ Request for Injunctive Relief. | 23 |
| J. Plaintiffs’ Allegations Against Belles Camp Communications, Inc. Plausibly State a Claim for Relief. | 24 |

| | | |
|------|--|----|
| K. | Plaintiffs’ Allegations Against Innovis Plausibly State a Claim for Relief. | 26 |
| L. | Plaintiffs’ Allegations Against the Zillow Defendants Plausibly State a Claim for Relief. | 27 |
| II. | INNOVIS’ AS-APPLIED FIRST AMENDMENT CHALLENGE FAILS. | 29 |
| III. | EXTRATERRITORIALITY DOES NOT BAR PLAINTIFFS’ CLAIMS AGAINST DEFENDANTS. | 32 |
| IV. | DEFENDANT INNOVIS’ PREEMPTION ARGUMENTS ARE MERITLESS AND BARRED. | 37 |
| A. | Whether Innovis Is Acting as a CRA is a Factual Issue. | 38 |
| B. | Daniel’s Law is Not Preempted by the FCRA. | 38 |
| C. | Daniel’s Law Does Not Interfere with FCRA’s Opt-Out System. | 43 |
| V. | DEFENDANTS CANNOT INVOKE IMMUNITY UNDER SECTION 230 OF THE COMMUNICATIONS DECENCY ACT. | 45 |
| A. | CDA Immunity is Not Established from Plaintiffs’ Complaints. | 46 |
| B. | Defendants Cannot Satisfy the Requirements for Section 230 Immunity. | 47 |
| VI. | PLAINTIFFS SHOULD HAVE THE OPPORTUNITY TO CORRECT ANY DEFICIENCIES. | 52 |
| | CONCLUSION..... | 52 |

TABLE OF AUTHORITIES

Cases

| | |
|--|------------|
| <i>Abrams v. eResearch Tech., Inc.</i> , 703 F. Supp. 3d 593 (E.D. Pa. 2023)..... | 36 |
| <i>Adams v. LexisNexis Risk & Info. Analytics Grp., Inc.</i> , 2010 WL 1931135 (D.N.J. May 12, 2010)..... | 26, 32, 40 |
| <i>Am. Boat Co. v. Unknown Sunken Barge</i> , 418 F.3d 910 (8th Cir. 2005) | 15 |
| <i>American Libraries Ass’n v. Pataki</i> , 969 F. Supp. 160 (S.D.N.Y. 1997) | 36 |
| <i>Anderson v. TikTok, Inc.</i> , 116 F.4th 180 (3d Cir. 2024) | 51 |
| <i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)..... | 5, 6 |
| <i>Atlas Data Priv. Corp. v. We Inform, LLC</i> , 758 F. Supp. 3d 322 (D.N.J. 2024)..... | 22, 31 |
| <i>Ball v. Kotter</i> , 723 F.3d 813 (7th Cir. 2013) | 15 |
| <i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007)..... | 6 |
| <i>Boring v. Google Inc.</i> , 362 F. App’x 273 (3d Cir. 2010) | 22 |
| <i>Borough of Keyport v. Maropakis</i> , 332 N.J. Super. 210 (App. Div. 2000)..... | 14 |
| <i>Bowley v. City of Uniontown Police Dep’t</i> , 404 F.3d 786 n.3 (3d Cir. 2005) | 30, 31 |
| <i>Brody v. Hankin</i> , 145 F. App’x 768 (3d Cir. 2005) | 46 |

| | |
|---|------------|
| <i>Brown v. U.S. Prob. Off.</i> , 2005 WL 2284207 (E.D. Tex. Aug. 15, 2005)..... | 20 |
| <i>Calabotta v. Phibro Animal Health Corp.</i> , 460 N.J. Super. 38 (2019)..... | 33 |
| <i>Calabria Ristorante, Inc. v. Ruggiero Seafood, Inc.</i> , 2023 WL 8643781 (D.N.J. Dec. 14, 2023)..... | 41 |
| <i>Carteret Properties v. Variety Donuts, Inc.</i> , 49 N.J. 116 (1967) | 14 |
| <i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983)..... | 23 |
| <i>Connelly v. Lane Const. Corp.</i> , 809 F. 3d 780 (3d Cir. 2016) | 25 |
| <i>Consumer Data Indus. Ass’n v. Frey</i> , 26 F.4th 1 (1st Cir. 2022)..... | 44 |
| <i>Consumer Data Indus. Ass’n v. Platkin</i> , 2024 WL 1299256 (D.N.J. Mar. 27, 2024) | 39, 41, 44 |
| <i>D’Agostino v. Johnson & Johnson, Inc.</i> , 133 N.J. 516 (1993) | 36, 37 |
| <i>Davenport v. Farmers Ins. Grp.</i> , 378 F.3d 839 (8th Cir. 2004) | 45 |
| <i>De Sole v. United States</i> , 947 F.2d 1169 (4th Cir. 1991) | 19 |
| <i>Doe v. Princeton University</i> , 30 F. 4th 335 (3d Cir. 2022) | 25 |
| <i>Duckett v. Clement Bros. Co.</i> , 375 F.2d 963 (6th Cir. 1967) | 19 |
| <i>Erie Ins. Co. v. Amazon.com, Inc.</i> , 925 F.3d 135 (4th Cir. 2019) | 49 |

| | |
|--|----------------|
| <i>F.T.C. v. Accusearch Inc.</i> , 570 F.3d 1187 (10th Cir. 2009) | 49, 51 |
| <i>Falcone v. Dickstein</i> , 92 F.4th 193 (3d Cir. 2024) | 24 |
| <i>Florida Star. Greater Philadelphia Chamber of Commerce v. City of Philadelphia</i> , 949 F.3d 116 (3d Cir. 2020) | 32 |
| <i>Foman v. Davis</i> , 371 U.S. 178 (1962)..... | 52 |
| <i>Freed v. Metro Mktg. Inc.</i> , 2013 WL 5466637 (D.N.J. Sept. 30, 2013)..... | 7 |
| <i>Galper v. JPMorgan Chase Bank, N.A.</i> , 802 F.3d 437 (2d Cir. 2015) | 45 |
| <i>Green v. America Online</i> , 318 F.3d 465 (3d Cir. 2003) | 50 |
| <i>Harris v. Patel</i> , 2018 WL 1128624 (D.N.J. Mar. 1, 2018) | 15 |
| <i>Henderson v. Source for Pub. Data, L.P.</i> , 53 F.4th 110 (4th Cir. 2022) | 49, 50 |
| <i>Hepp v. Facebook</i> , 14 F.4th 204 (3d Cir. 2021) | 48 |
| <i>Huggins v. FedLoan Servicing</i> , 2020 WL 13645747 (D.N.J. Dec. 2, 2020)..... | 22 |
| <i>In re Insulin Pricing Litig.</i> , 2024 WL 5252471 (D.N.J. Dec. 31, 2024)..... | 36 |
| <i>In re: Daniel’s Law Compliance Litigation</i> , 2024 WL 4905924 (D.N.J. Nov. 26, 2024) | 18 |
| <i>Individual Reference Servs. Group, Inc. v. Federal Trade Comm’n</i> , 145 F. Supp. 2d 6 (D.D.C. 2001)..... | 26, 32, 39, 40 |

| | |
|--|----|
| <i>Instructional Sys., Inc. v. Computer Curriculum Corp.</i> , 35 F.3d 813 (3d Cir. 1994) | 36 |
| <i>Katz v. Ambit Ne., LLC</i> , 2020 WL 5542780 (D.N.J. Sept. 16, 2020) | 6 |
| <i>Kellman v. Spokeo, Inc.</i> , 599 F. Supp. 3d 877 (N.D. Cal. 2022) | 51 |
| <i>Kennell v. Gates</i> , 215 F.3d 825 (8th Cir. 2000) | 15 |
| <i>Kratovil v. City of New Brunswick</i> , 2024 WL 1826867 (N.J. App. Div. Apr. 26, 2024) | 35 |
| <i>Krause, v. RocketReach, LLC</i> , 561 F. Supp. 3d 778 (N.D. Ill. Sept. 21, 2021) | 46 |
| <i>Lexmark Int'l, Inc. v. Static Control Components, Inc.</i> , 572 U.S. 118 (2014) | 20 |
| <i>Lukis v. Whitepages Inc.</i> , 454 F. Supp. 3d 746 (N.D. Ill. 2020) | 51 |
| <i>Lum v. Bank of Am.</i> , 361 F.3d 217 (3d Cir. 2004) | 30 |
| <i>Lupian v. Joseph Cory Holdings LLC</i> , 905 F.3d 127 (3d Cir. 2018) | 37 |
| <i>Mayer v. Belichick</i> , 605 F. 3d 223 (3d Cir. 2010) | 16 |
| <i>McDonnell v. State of Ill.</i> , 163 N.J. 298 (N.J. 2000) | 37 |
| <i>Mehlman v. Mobil Oil Corp.</i> , 153 N.J. 163 (1998) | 34 |
| <i>Moretti v. Hertz Corp.</i> , 2017 WL 1032783 (D. Del. Mar. 17, 2017) | 46 |

| | |
|--|--------|
| <i>MSP Recovery Claims, Series, LLC v. Sanofi-Aventis U.S. LLC</i> , 2020 WL 831578 (D.N.J. Feb. 20, 2020) | 9 |
| <i>Murray-Nolan v. Rubin</i> , No. WL 4104343 (D.N.J. Sept. 8, 2022) | 24 |
| <i>New Jersey Carpenters & the Trs. Thereof v. Tishman Const. Corp. of New Jersey</i> , 760 F.3d 297 (3d Cir. 2014) | 6, 17 |
| <i>Oxford Consumer Discount Co. of North Philadelphia v. Stefanelli</i> , 102 N.J. Super. 549 (1968) | 34 |
| <i>Pace v. Baker-White</i> , 432 F. Supp. 3d 495 (E.D. Pa. 2020) | 51, 52 |
| <i>Peikin v. Kimmel & Silverman, P.C.</i> , 576 F. Supp. 2d 654 (D.N.J. 2008) | 36 |
| <i>Phillips v. County of Allegheny</i> , 515 F.3d 224 (3d Cir. 2008) | 6, 9 |
| <i>Pladeck v. Credit Suisse First Fin. Corp.</i> , 2024 WL 4601461 (D.N.J. Oct. 29, 2024) | 42 |
| <i>Portage Shoe Mfg. Co. v. Reich</i> , 53 N.J. Super. 600 (App. Div. 1959) | 14 |
| <i>Prime Property & Cas. Ins. Inc. v. Freightway Logistics LLC</i> , 2019 WL 6907532 (D.N.J. Dec. 19, 2019) | 30 |
| <i>Progressive Spine Orthopaedics LLC v. Empire Blue Cross Blue Shield</i> , 2017 WL 751851 (D.N.J. Feb 27, 2017) | 10 |
| <i>Real v. Radir Wheels, Inc.</i> , 198 N.J. 511 (2009) | 33 |
| <i>Red Hawk Fire & Sec., LLC v. Siemens Indus. Inc.</i> , 449 F. Supp. 3d 449 (D.N.J. 2020) | 38 |
| <i>Richmond Med. Ctr. for Women v. Herring</i> , 570 F.3d 165 (4th Cir. 2009) | 29 |

| | |
|--|----------------|
| <i>Santiago v. Warminster Twp.</i> , 629 F.3d 121 (3d Cir. 2010) | 7 |
| <i>Schulman v. Zoetis, Inc.</i> , 684 F. Supp. 3d 275 (D.N.J. 2023) | 33 |
| <i>Seamans v. Temple Univ.</i> , 744 F.3d 853 (3d Cir. 2014) | 42 |
| <i>Sixth Angel Shepherd Rescue Inc. v. West</i> , 477 F. App'x 903 (3d Cir. 2012) | 24 |
| <i>Sixth Angel Shepherd Rescue Inc. v. West</i> , 790 F. Supp. 2d 339 (E.D. Pa. 2011) | 24 |
| <i>Snowdy v. Mercedes-Benz USA, LLC</i> , 2024 WL 1366446 (D.N.J. Apr. 1, 2024) | 23 |
| <i>State v. Worthy</i> , 141 N.J. 368 (1995) | 34 |
| <i>Stephenson v. AT&T Servs., Inc.</i> , 2021 WL 3603322 (E.D. Pa. Aug. 13, 2021) | 15 |
| <i>Tjokrowidjojo v. San Lucas</i> , 2021 WL 1143379 (E.D. Pa. Mar. 25, 2021) | 22 |
| <i>Trans Union LLC v. FTC</i> , 295 F.3d 42 (D.C. Cir. 2002) | 26, 32, 39, 40 |
| <i>Turner v. Aldens, Inc.</i> , 179 N.J. Super. 596 (App. Div. 1981) | 33, 35 |
| <i>Victaulic Co. v. Tieman</i> , 499 F.3d 227 (3d Cir. 2007) | 30, 47 |
| <i>Vidal v. Elster</i> , 602 U.S. 286 (2024) | 48 |
| Statutes | |
| 15 U.S.C. § 1681a(f) | 29 |
| 15 U.S.C. § 1681b | 43, 44 |

| | |
|---------------------------------------|--------------|
| 15 U.S.C. § 1681c | 42 |
| 15 U.S.C. § 1681c(d) | 31, 39 |
| 15 U.S.C. § 1681t(a) | 39, 45 |
| 15 U.S.C. § 1681t(b) | 40 |
| 18 U.S.C. § 1681b(a) | 29 |
| 47 U.S.C. § 230 | passim |
| N.J.S.A. § 56:8-166.1(a) | passim |
| N.J.S.A. § 56:8-166.1(b) | 4 |
| N.J.S.A. § 56:8-166.1(d) | 4, 7, 27, 49 |
| N.J.S.A. § 56:8-166.3 | 35, 36 |
| N.J.S.A. § 56:8-166.4 | 34 |
| New Jersey Law P.L. 2015, c.226 | 13 |
| New Jersey Law P.L. 2021, c.371 | 13 |
| New Jersey Law P.L. 2023, c.113 | 13 |

Other Authorities

| | |
|--|--------|
| <i>The Fair Credit Reporting Act’s Limited Preemption of State Laws</i> , 87 Fed. Reg. 41,042 (Jul. 11, 2022) | 39, 43 |
|--|--------|

Rules

| | |
|-------------------------|--------|
| F.R.C.P. 12(b)(6) | Passim |
|-------------------------|--------|

PRELIMINARY STATEMENT

Defendants’ consolidated motion to dismiss under Rule 12(b)(6) quibbles with Plaintiffs’ Complaints but principally contains a myriad of recycled legal arguments which have been rejected time and again by multiple courts. Each of those arguments fail because of the well-pled factual allegations of the Complaints, as a matter of law or because they are simply premature. As a result, Defendants’ applications to dismiss Plaintiffs’ Daniel’s Law claim in these actions fail.

Claims under New Jersey’s Daniel’s Law, N.J.S.A. 56:8-166.1, are straightforward and support the law’s purpose “to prevent further attacks on certain government officials and their families” which courts have confirmed is a compelling “government interest of the highest order.” Individuals who are entitled to protection under the law—judges, prosecutors, law enforcement and their families—can effectuate their rights by sending written notice to a person, business or association (*id est*, data brokers) advising that the individual is a covered person under Daniel’s Law and notifying the data broker to cease disclosure, re-disclosure or otherwise making available the individual’s home address, including street address, and unpublished home telephone number, including cell phone number. Upon receipt the data broker has ten business days within which to comply. If it negligently does not, then it is liable to the individual or their assignee.

Plaintiffs' detailed Complaints clearly identify allegations sufficient to establish each element of a Daniel's Law claim. Covered persons used a technology platform to send written non-disclosure requests to Defendants via email seeking to cease disclosure of protected information under Daniel's Law. Defendants did not comply within ten business days, at the time the Complaints were filed, and in some cases, even as of today. Many of those covered persons' claims were then assigned to Atlas (consistent with the law), and Atlas, along with several individuals, then filed these actions.

Because each of these facts and more have been explained in significant detail in the Complaints, Plaintiffs have met their minimal burden to plead facts supporting the elements of a Daniel's Law claim. Accordingly, Defendants' principal argument that their liability is not sufficiently pleaded should be rejected. In addition, certain defendants' arguments for preemption under the Fair Credit Reporting Act, seeking invalidation (again) under the First Amendment, or arguing that Daniel's Law does not apply to persons, businesses or associations outside of New Jersey, similarly lack merit. And additional as-applied challenges or claims of immunity under the Communications Decency Act are premature and require findings on contested facts related to those Defendants' operations that are procedurally improper on a 12(b)(6) motion. As a result, and as set forth in detail below, Defendants' motions to dismiss Plaintiffs' Complaints should be denied.

FACTUAL BACKGROUND

A. Daniel’s Law.

Daniel’s Law was enacted in response to the tragic murder of the son of a New Jersey federal Judge, who was killed by a gunman who found the home addresses of his victims from companies, like defendants, that readily make that information available on the internet. Compl. ¶¶ 5–8.¹ Daniel’s Law seeks to safeguard the personal information of current and former judges, prosecutors, law enforcement officers, prosecutors, and their eligible family members (i.e., “Covered Persons”), by providing a comprehensive statutory framework for Covered Persons to prohibit and enforce persons, businesses, associations and government from disclosing, re-disclosing, or otherwise making available their home addresses or unpublished home telephone numbers. *Id.* ¶ 9. Within ten business days of receiving a written nondisclosure request from a Covered Person,² private persons and organizations must cease to “solicit, sell, manufacture, give, provide, lend, trade, mail, deliver, transfer, post, publish, distribute, circulate, disseminate, present, exhibit, advertise,

¹ Unless stated otherwise, “Compl.” refers to the Complaint filed in *Atlas Data Privacy Corp., et al. v. DM Group Inc., et al.*, No. 24-cv 04075-HB, Dkt. No. 1.

² While requests are to be transmitted by “Authorized Persons”, that definition is not relevant here because (a) a Covered Person is an Authorized Person under the law, and (b) all non-disclosure requests here were sent to defendants by the Covered Persons themselves. See N.J.S.A. § 56:8-166.1(a)(2) and Compl. ¶¶ 45-46.

or offer,” or otherwise “make[] available or viewable within a searchable list or database,” that Covered Person’s protected information. *Id.*

Daniel’s Law provides a clear enforcement mechanism for Covered Persons to vindicate their rights and expressly authorizes the use of assignments: “[a] person, business, or association that violates [Daniel’s Law] shall be liable to the covered person *or the covered person’s assignee*, who may bring a civil action in the Superior Court.” N.J.S.A. § 56:8-166.1(b) (emphasis added). “Assignee” is defined as “a person or entity to whom or which an authorized person has assigned, in writing, a covered person’s right to bring a civil action for a violation of [Daniel’s Law].” *Id.* § 56:8-166.1(d). Given the importance of compliance, it should not be surprising that organizations failing to timely comply with a Covered Person’s nondisclosure request are subject to statutory penalties for their negligence. *Id.* § 56:8-166.1(c)-(1) (“The court shall award ... actual damages, but not less than liquidated damages computed at the rate of \$1,000 for each violation of this act.”).

B. Defendants Violated Daniel’s Law By Failing to Timely Comply with the Nondisclosure Requests.

All of the moving Defendants are businesses or associations that violated Daniel’s Law by disclosing, re-disclosing, or otherwise making available the personal information of Covered Persons more than ten business days after receiving nondisclosure requests. *See, e.g.,* Compl. ¶¶ 47–48, 54–55. Using the Atlas platform,

the Covered Persons in these actions³ selected the Defendants and sent one or more written nondisclosure requests to each of them. *Id.* ¶¶ 45–46. In each request, the Covered Persons advised that they are a covered person as defined by Daniel’s Law, and that they sought to effectuate their privacy rights under the law by having that Defendant cease disclosure of specific protected information listed in the nondisclosure request. *See id.* The Covered Persons assigned their claims to Atlas (*id.* ¶¶ 20, 24, 49), and Plaintiffs filed these actions because Defendants failed to comply with the nondisclosure requests within the requisite statutory ten business days, and in many cases, continue to disclose the home addresses and phone numbers of these Covered Persons in defiance of the clear mandate of this State. *Id.* ¶¶ 30, 47–50, 57.

ARGUMENT

I. DEFENDANTS’ LIABILITY UNDER DANIEL’S LAW IS SUFFICIENTLY PLEADED.

To withstand Defendants’ motion to dismiss pursuant to 12(b)(6), Plaintiffs’ Complaints need only “contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Plaintiffs satisfy this “plausibility” standard by pleading “factual content that

³ The covered persons in these actions include both the individual plaintiffs who did not assign their rights to Atlas (the “Individual Plaintiffs”) and also covered persons who assigned their rights to Atlas (defined in the complaints as “Covered Persons”).

allows the court to draw the *reasonable inference* that the defendant is liable for the misconduct alleged.” *Id.* (emphasis added). The pleading burden is not onerous—Plaintiffs need only state enough facts to “suggest the required elements” or “raise a reasonable expectation that discovery will reveal evidence” supporting those elements. *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 55 (2007); *Phillips v. County of Allegheny*, 515 F.3d 224, 234 (3d Cir. 2008).

Even though the Court must “accept all factual allegations in the complaint as true and draw all reasonable inferences in favor of the plaintiff[s],” *New Jersey Carpenters & the Trs. Thereof v. Tishman Const. Corp. of New Jersey*, 760 F.3d 297, 302 (3d Cir. 2014), Defendants demand that the Court read every factual allegation in the most contrived and narrow light. Defendants argue that Plaintiffs omit material factual allegations including, “how many [takedown notices] were received”; “when the statutory period for compliance began to run or when it expired”; and “what Protected Information a Defendant possessed before a takedown notice was sent” (*see* Mot. 14)—but Plaintiffs are not required to plead their Complaints with this level of specificity. This is not a fraud case where a Rule 9 heightened pleading standard applies. *C.f. Katz v. Ambit Ne., LLC*, No. 3:20-CV-1289-BRM-DEA, 2020 WL 5542780, at *2 (D.N.J. Sept. 16, 2020) (heightened standard requires “the ‘who, what, when, where and how’ of the events at issue.”). In any event, Plaintiffs *do* actually allege many facts concerning the “who, what,

when, where and how” of Defendants’ Daniel’s Law violations, and Plaintiffs provide more than sufficient information to allow Defendants to form defenses, seek discovery, and proceed with litigation—much like the dozen cases that raised similarly doomed arguments and are being litigated in New Jersey state courts.

On this motion, the Court should: (1) “tak[e] note of the elements a plaintiff must plead to state a claim;” (2) identify “those allegations that are no more than conclusions and thus not entitled to the assumption of truth;” and (3) “where there are well-pleaded factual allegations . . . assume their veracity and then determine whether they plausibly give rise to an entitlement for relief.” *Santiago v. Warminster Twp.*, 629 F.3d 121, 130 (3d Cir. 2010); *Freed v. Metro Mktg. Inc.*, No. CIV.A. 12-6201 JAP, 2013 WL 5466637, at *2 (D.N.J. Sept. 30, 2013).

To assist the Court with this analysis, the chart below sets forth the elements of Daniel’s Law and the corresponding factual allegations in Plaintiffs’ Complaints:

| Daniel’s Law Elements | Plaintiffs’ Allegations (emphases added) |
|---|--|
| “An authorized person”; ⁴ N.J.S.A. § 56:8-166.1(a)(2) | The Individual Plaintiffs and Covered Persons are covered persons. Compl. ¶¶ 15–18 (Individual Plaintiffs are covered persons); <i>id.</i> ¶ 20 (Covered Persons are “19,532 individuals who are all ‘covered persons’ under Daniel’s Law”); <i>see also</i> |

⁴ A “covered person” is an “authorized person” in addition to someone expressly identified in N.J.S.A. §56:8-166.1(d)(1), (2), or (3), who is acting on behalf of a covered person. N.J.S.A. §56:8-166.1(d).

| | |
|--|---|
| | <i>id.</i> ¶¶ 21, 26, 28 (explaining how Covered Persons’ provide confirmation of their eligibility through Atlas’ platform). |
| “shall provide written notice to the person from whom the authorized person is seeking nondisclosure”; N.J.S.A. § 56:8-166.1(a)(2) | “[E]ach of the Individual Plaintiffs and all of the Covered Persons (who assigned claims to Atlas) <i>sent Defendants written nondisclosure requests (via email)</i> in accordance with Daniel’s Law, using AtlasMail.” Compl. ¶ 45. |
| “written notice” shall state they are an “authorized person”; N.J.S.A. § 56:8-166.1(a)(2) | The written notice (in the form of an email) stated, in part: “ <i>I am a ‘Covered Person’</i> as defined by New Jersey Law” Compl. ¶ 46. |
| “request[] that the person cease the disclosure of the information and remove the protected information from the Internet or where otherwise made available.” N.J.S.A. § 56:8-166.1(a)(2) | The written notice (in the form of an email) stated, in part: “I hereby <i>request that you not disclose or re-disclose</i> on the Internet or otherwise make available, the following <i>protected information</i>” Compl. ¶ 46. |
| “Upon notification ... and not later than 10 business days following receipt thereof”; N.J.S.A. § 56:8-166.1(a)(1) | The written notices were sent “on or about <i>January 7, 2024</i> ” (Compl. ¶ 45) and “Defendants <i>failed to cease the disclosure or re-disclosure ... within the time period required by Daniel’s Law</i> ” (<i>id.</i> ¶ 47) and “[e]ven as of the date of this filing, Defendants still refuse to comply with Daniel’s Law” (<i>id.</i> ¶ 48). |

| | |
|--|--|
| <p>“shall not disclose or re-disclose on the Internet or otherwise make available the home address or unpublished home telephone number of any covered person”;</p> <p>N.J.S.A. § 56:8-166.1(a)(1)</p> | <p>“The <i>protected information [including home addresses and/or unpublished home telephone numbers]</i> of the Individual Plaintiffs and the Covered Persons <i>remains ‘available or viewable within a searchable list or database’ or otherwise made available</i>” (Compl. ¶54) and “Defendants <i>did not cease</i> the disclosure” (<i>id.</i> ¶ 55).</p> |
|--|--|

Properly assuming the truth of Plaintiffs’ allegations and drawing all reasonable inferences in favor of Plaintiffs, *see Phillips*, 515 F.3d at 233, it is clear Plaintiffs have satisfied their pleading burden and these cases should proceed.

A. The Complaints Plausibly Plead Facts Related to Assignments.

Defendants’ contention that Plaintiffs should have included more details regarding the assignments (Mot. at 17–18) is a meritless argument that many courts have rejected. It is sufficient to plead, as Plaintiffs have, that Atlas was assigned rights for the Covered Persons. *See, e.g., MSP Recovery Claims, Series, LLC v. Sanofi-Aventis U.S. LLC*, No. 318CV2211BRMLHG, 2020 WL 831578, at *7 (D.N.J. Feb. 20, 2020) (denying motion to dismiss and holding that “many other district courts across the country have not required plaintiffs to add detailed allegations at this stage to assert claims for all assignors”). Defendants’ demand that Plaintiffs include additional details regarding the identity of each of the Covered Persons and their assignments in a public pleading is not required under 12(b)(6) and

is contrary to the protections afforded by the New Jersey Legislature under Daniel's Law. Defendants' reliance on *Progressive Spine Orthopaedics LLC v. Empire Blue Cross Blue Shield*, Civ. Act. No. 16-01649, 2017 WL 751851 (D.N.J. Feb 27, 2017) is misplaced as it deals with ERISA-specific assignment-pleading requirements that have no relation to the present case. Indeed, this exact same argument has been raised several times, and every court to consider the argument (raised by Defendants here) has agreed with Plaintiffs and either upheld the sufficiency of the Complaints or upheld it on the condition that Atlas produce a Covered Persons/Assignments list under the protection of a protective order.⁵ Defendants' argument is truly illusory given that all Defendants here already have the list of Covered Persons, as well as Atlas' Daniel's Law Terms of Service and Assignment Confirmation exemplar⁶.

⁵ See, e.g., Certification of Rajiv D Parikh, Esq. ("Parikh Cert.") at Exs. A-D (*Atlas Data Privacy Corp., et al. v. REIPro*, Transcript of Hearing on Motion to Dismiss at 75:17-22, 76:24-77:2; *Atlas Data Privacy Corp., et al. v. Attom Data*, MER-L-273-24, Transcript of Hearing on Motion to Dismiss at 16 ("And here it is clear to me, after going through the complaint many times, that they plead sufficient facts to show that the assignors are covered persons under Daniel's Law and -- and in fact have standing."); *Atlas Data Privacy Corp., et al. v. CheckPeople, LLC, et al.*, MON-L-506-24, Order Denying Motion to Dismiss (rejecting arguments on motion to dismiss that Atlas lacks standing to bring its claims based on assignments); *Atlas Data Privacy Corp., et al. v. Batchservice, LLC, et al.*, MON-L-485-24, Order Denying Motion to Dismiss (rejecting arguments on motion to dismiss that Atlas lacks standing to bring its claims based on assignments)).

⁶ For all but five defendants, Plaintiffs produced these documents in May 2024, as discussed at the April 18, 2024 status conference. For five defendants, whose cases were removed after May 2024, Plaintiffs produced these documents prior to filing this brief.

Plaintiffs will in discovery again provide that assignment information to all Defendants.

B. The Complaints Plausibly Allege that the Individual Plaintiffs and Covered Persons Sent Their Own Notices.

As stated in the Complaints, *the Individual Plaintiffs and Covered Persons* sent their written notices using Atlas’s AtlasMail email service. *See, e.g.,* Compl. ¶¶ 45–46. Defendants’ argument that Atlas was not an “authorized person” is irrelevant because the written nondisclosure requests were sent by the Covered Persons and at no point do the Complaints suggest that Atlas was the sender of these requests.

The fact that these individuals used AtlasMail to send these nondisclosure requests (as opposed to Google’s Gmail or Microsoft Outlook) does not somehow make *Atlas* the one who sent the takedown notices. *See* Mot. 19–20. Defendants’ meritless argument is essentially that if a Covered Person sent a nondisclosure request via the mail service of a common carrier such as FedEx or UPS, that the carrier would be the sender of that request. The fact that Atlas offered an individualized email service that Covered Persons entrusted to *deliver* the written nondisclosure requests here does not make Atlas the sender of those emails any more than FedEx or UPS is the sender of all the mail and packages they deliver. Nor does the fact that Atlas tells its users that it may schedule the delivery to realize certain efficiencies make Atlas the sender of the email.

Critically, nothing in the terms of service entitles Atlas to make the decision to send a nondisclosure request to any business or association on behalf of anyone. *See generally* Atlas Terms of Service, “Sending Takedown Notices.”⁷ It is always the user who decides whether to send a nondisclosure request to any business or association, and it is always the user who is the sender. The terms of service and Atlas’s system give covered persons the ability to send nondisclosure requests with immediate delivery or give Atlas the discretion to efficiently deliver requests in accordance with its systems’ capabilities. Viewing all allegations of the Complaints in favor of Plaintiffs, they have adequately pled that covered persons sent written nondisclosure requests to Defendants, and the motion to dismiss on this ground should be denied.

C. The Complaints Plausibly Allege Facts Establishing that the Nondisclosure Requests were Legally Sufficient.

The Complaints detail how the nondisclosure requests complied with all legal requirements of Daniel’s Law and were, accordingly, legally sufficient. Daniel’s Law provides that an authorized person “shall provide written notice to the person from whom the authorized person is seeking nondisclosure that the authorized person is an authorized person and requesting that the person cease the disclosure of the information and remove the protected information from the Internet or where

⁷ Attached as Exhibit A to Declaration of Angelo A. Stio III, Dkt. 59-3.

otherwise made available.” N.J.S.A. § 56:8-166.1(a)(2). As required by Daniel’s Law, the exemplar notice provided in the Complaints is (1) written; (2) indicates the sender is an authorized person (“I am a ‘Covered Person’ as defined by New Jersey Law P.L. 2023, c.113, P.L.2021, c.371”); (3) states that the Covered Person is requesting the nondisclosure on the Internet or where otherwise made available; and (4) identifies the specific protected information (the Covered Person’s name and address or name and phone number) for which non-disclosure is sought. *See* Compl. ¶ 46.

Helpfully, the exemplar notice included in the Complaints also clearly specifies the laws of New Jersey under which the notice is made and incorporates the language of the cited statutes themselves by reference. *See* Compl. ¶ 46 (“Pursuant to the Act and Section 3 of New Jersey P.L. 2015, c.226 (C.56:8-166.1), I hereby request that . . .”). Because the Legislature specified the form and contents of the notice, and because the Complaints’ exemplar notice complies with the Legislature’s specifications, the notice is sufficient as a matter of law. These notices were identical in form, indeed *helping* Defendants to identify their obligations under Daniel’s Law to effectuate compliance. Yet Defendants complain that these uniform nondisclosure requests impeded their compliance. That makes no sense.

Defendants improperly rely on cases espousing the New Jersey rule that “[i]n the absence of express provision, the form and contents of a notice required by a

statute are dependent upon the wording of the statute construed in the light of its intent and purpose.” *Borough of Keyport v. Maropakos*, 332 N.J. Super. 210 (App. Div. 2000) (emphasis added) (quoting *Portage Shoe Mfg. Co. v. Reich*, 53 N.J. Super. 600, 605, 148 A.2d 47 (App. Div. 1959)). As Defendants’ cases demonstrate, when the form and contents of a notice required by statute are provided by legislature, the statute controls. *See, e.g., Carteret Properties v. Variety Donuts, Inc.*, 49 N.J. 116, 124 (1967) (concerning the sufficiency of a notice where the governing statute required the notice to “‘specify’ the cause of the termination of the tenancy”); *C.f. Borough of Keyport*, 332 N.J. Super. 210, 221 (App. Div. 2000) (concerning form and content of notice where governing statute did not specify the contents of the notice). Defendants’ reliance on *Carteret* and *Borough* is misplaced insofar as Daniel’s Law specifies the content of the required notice, and the notices sent here contain information required under the statute.

D. The Complaints Plausibly Allege Facts Establishing that Defendants Received the Written Notices Sent to Them.

Defendants’ argument that Plaintiffs somehow fail to plausibly allege that Defendants received the written notices (Mot. at 25–26) fails under the law.⁸ The Complaints allege that “each of the Individual Plaintiffs and all of the Covered

⁸ Any assertion by a Defendant that it did not receive nondisclosure requests from the Covered Persons would be properly explored in discovery into Defendant’s email systems, policies and practices.

Persons ... sent Defendants written nondisclosure requests (via email) ... using AtlasMail.” Compl. ¶¶ 45, 28. An allegation that an email was sent to a particular recipient necessarily presumes that the email was received by that recipient. *See Stephenson v. AT&T Servs., Inc.*, No. CV 21-0709, 2021 WL 3603322, at *5 (E.D. Pa. Aug. 13, 2021) (holding that there is a rebuttable presumption that emails sent have reached their intended destination); *see also Ball v. Kotter*, 723 F.3d 813, 830 (7th Cir. 2013) (finding that a presumption existed that emails were properly sent, received, and read); *Am. Boat Co. v. Unknown Sunken Barge*, 418 F.3d 910, 914 (8th Cir. 2005) (“[w]e agree with the district court that a presumption of delivery should apply to e-mails”); *Kennell v. Gates*, 215 F.3d 825, 829 (8th Cir. 2000) (holding that a jury would be able to make the same inference of receipt regarding information sent via electronic mail as it would for information sent via the postal service); *see also* Parikh Cert. at Ex. A, Transcript of Hearing on Motion to Dismiss in *Atlas, et al. v. REIPro, LLC, et al.*, MRS-L-000231-24, at 64:21-66:4 (ruling that plaintiffs’ allegation that the covered persons sent emails providing written notice was sufficient to allege that defendant received written notice on the same day the emails were sent). Plaintiffs’ allegations regarding email delivery should be taken as true. *Harris v. Patel*, 2018 WL 1128624 (D.N.J.Mar. 1, 2018), at *1. Given the presumption of email delivery and receipt recognized by courts, Plaintiffs plausibly allege Defendants received the nondisclosure requests.

E. Plaintiffs Plausibly Allege that Defendants Possessed and Disclosed Protected Information.

In another tortured reading of the Complaints, Defendants argue that there is no express allegation that Defendants possessed the protected information in the first instance. Mot. at 27–28. This argument again ignores the requirement that the Court construe the Complaints in the light favorable to the plaintiffs, to determine whether relief is available “*under any reasonable reading*” of the Complaints. *Mayer v. Belichick*, 605 F. 3d 223, 229 (3d Cir. 2010) (emphasis added). There is no plausible reading of the Complaints that supports Defendants’ argument. The Complaints allege that: (i) each Defendant “is an entity that discloses ... home addresses and/or unpublished home telephone numbers of covered persons” (Compl. ¶ 31); (ii) the nondisclosure requests expressly identified the protected information that each Defendant should remove (*see, e.g., id.* ¶ 46); (iii) “Defendants *did not cease* the disclosure or re-disclosure on the Internet or the otherwise making available of information as required under Daniel’s Law” (*id.* ¶ 55 (emphasis added)); and (iv) “[e]ven as of the date of this filing ... Protected information of the Individual Plaintiffs and those Covered Persons ... *remains available from Defendants using Defendants’ search tools or other means of disclosure*” (*id.* ¶ 48 (emphasis added)). From the allegation that Defendants “*did not cease*” disclosure, the Court can and should reasonably infer that the Protected Information was (and still is) in Defendants’ possession and was being disclosed, re-disclosed, or otherwise made

available as of the filing of the complaint.⁹ *New Jersey Carpenters*, 760 F.3d 297, 302 (“A court must accept all factual allegations in the complaint as true and draw all reasonable inferences in favor of the plaintiff.”).¹⁰ There is no requirement that Plaintiffs detail that protected information in the Complaints, which will be provided in discovery. The full extent of Defendants’ violations is something that will be determined based on discovery obtained from Defendants, not the pleadings.

Defendants’ argument that the Complaints fail to allege the particular protected information Defendants possessed about the Individual Plaintiffs or Covered Persons is also refuted by the plain language of the Complaints: “[Defendant] is an entity that discloses...*home addresses* and/or *unpublished home telephone numbers* of covered persons.” Compl., ¶31. No further specificity is required at this pleading stage.

F. The Complaints Plausibly Allege Defendants’ Culpability.

Defendants’ suggestion that Plaintiffs needed to include more factual allegations regarding their culpability is also meritless. When Plaintiffs filed these

⁹ Defendants’ reliance on the Order Denying the Motion to Dismiss in *Atlas, et al. v. Spycloud, et al.*, MRS-L-000263-24, is misleading. In no way did the *Spycloud* court find that Plaintiffs’ allegations were insufficient to state a claim for relief. To the contrary, the court’s order indicated, “At this juncture, the court only addresses personal jurisdiction.” See *Spycloud* Order Denying Motion to Dismiss, at 8.

¹⁰ Additionally, Defendants’ reliance on Atlas’ Terms of Service disclaimer (see Mot. at 28) does not negate the allegations in the Complaints.

Complaints, this Court had not yet issued its ruling regarding the minimum degree of culpability necessary to assert a claim under Daniel’s Law. In asserting these claims, however, Plaintiffs included factual allegations that can and should be read to establish, at a minimum, that Defendants’ disclosure of protected information ten business days following their receipt of written nondisclosure requests was the result of their negligence. As this Court held, “Daniel’s Law must be read as imposing liability only if a defendant *unreasonably* disclosed or made available the home addresses and unlisted telephone numbers of covered persons after the statutory deadline had expired.” *In re: Daniel’s Law Compliance Litigation*, No. CV 24-10600, 2024 WL 4905924, at *12 (D.N.J. Nov. 26, 2024) (emphasis added). The Complaints plead that Defendants are disclosing, re-disclosing, or otherwise making available protected information “without sufficient regard for the risks and consequences imposed upon individuals who serve critical judicial and law enforcement roles.” Compl. ¶ 2. The Complaints further plead that Defendants “wantonly and repeatedly disregard the law” and “demonstrate a callousness towards the well-being of those who serve.” *Id.* ¶ 3. The whole purpose of Daniel’s Law is to protect Covered Persons, with resulting liability for those companies that continue to disclose protected information “without sufficient regard to the risks and consequences imposed on individuals.” *Id.* ¶ 35. The Complaints further plead that Defendants failed to remove protected information after covered persons’ demands.

Id. ¶¶ 45-57. Together, these factual allegations when assumed to be true demonstrate Defendants’ obligations under Daniel’s Law, their failures and, as a result, their culpability for acting “without sufficient regard for the risks” of their failure to comply with the law. *See, e.g., Duckett v. Clement Bros. Co.*, 375 F.2d 963, 964 (6th Cir. 1967) (holding a “charge of negligence could easily be distilled from the complaint’s language,” even though the “complaint did not use the word ‘negligence’ in describing the alleged tortious conduct” because the “complaint did describe the conduct of the defendant in strong and condemnatory language.”); *De Sole v. United States*, 947 F.2d 1169, 1178 (4th Cir. 1991) (“The mere failure to include the words ‘gross negligence’ in the complaint does not bar such a claim at the 12(b)(6) stage when combined with the facts present in the record.”). The extent of Defendants’ culpability—negligence, reckless disregard or willfulness—is something that will be determined based on discovery from Defendants. Nothing more was required at this pleadings stage.

G. Plaintiffs’ Allegations Plausibly Establish Causation.

Defendants contend that Plaintiffs must allege specific safety risks to Covered Persons resulting from each Defendant’s specific statutory violation to establish causation. Mot. at 35. But the question of proximate cause “is controlled by the nature of the statutory cause of action”, addressing “whether the harm alleged has a sufficiently close connection to the conduct the statute prohibits.” *Lexmark Int’l, Inc.*

v. Static Control Components, Inc., 572 U.S. 118, 133 (2014). Unlike certain other privacy statutes, Daniel’s Law does not require that the unlawful disclosure serve as a proximate cause of some additional harm—beyond the harm of disclosure itself—to establish a claim.¹¹ The plain text of the statute does not require proof that the disclosure caused an increased safety risk, nor any other additional harm such as economic loss or reputational harm. A covered person need only establish that the recipient of the takedown notice failed to cease its disclosure “on the Internet or otherwise” of “the home address or unpublished home telephone number of” the covered person within ten business days. N.J.S.A. § 56:8-166.1(a)(1).

The Complaints allege exactly that. They assert that: (1) the covered persons sent written nondisclosure requests regarding their protected personal information to each Defendant, (2) which failed to timely comply and remained noncompliant as of the date the Complaints were filed, such that (3) the covered persons’ “protected information (including home addresses and/or unpublished home telephone numbers) of the Individual Plaintiffs and Covered Persons continues to be disclosed, re-disclosed or otherwise made available” *by Defendants*.

¹¹ For example, “[t]o establish a violation of the accuracy provision of the [federal] Privacy Act, plaintiff must show” a failure to maintain accurate records, an adverse determination by the Bureau of Prisons, and that “the Bureau of Prisons’ reliance on the inaccurate records was the proximate cause of the adverse determination.” *Brown v. U.S. Prob. Off.*, 2005 WL 2284207, at *2 (E.D. Tex. Aug. 15, 2005). Daniel’s Law, by contrast, does not require an adverse event resulting from the unlawful disclosure.

As for Defendants’ contention that the protected information was not public “much less that any Defendant disclosed such information to any third party more than ten business days after receiving a takedown request,” (Mot. at 35), such arguments simply ignore the foregoing allegations. To the extent Defendants insist that specific phone numbers were public prior to their disclosures, this goes to the ultimate burden of proof—not the sufficiency of the pleadings. Taking all reasonable inferences in favor of Plaintiffs, as required on a Rule 12(b)(6) motion, Plaintiffs’ allegations are sufficient to plead proximate cause.

H. Plaintiffs Have Alleged Damages.

Defendants’ challenge as to damages also fails. Daniel’s Law provides that the court “shall award ... actual damages,” N.J.S.A. § 56:8-166.1 (c)(1), and “shall award ... punitive damages upon proof of willful or reckless disregard of the law” N.J.S.A. § 56:8-166.1(c)(2). Here, the Complaints outline the genesis of Daniel’s Law resulting from the murder of a Judge’s son and the murders, attacks and threats to covered persons resulting from disclosure of their protected information. Compl. ¶¶ 1–4. The Complaints also outlined exemplar stories of harm to Plaintiffs including fire bombings and armed gunmen at their homes. *Id.* ¶¶ 15–18. From these allegations, the Court can reasonably infer the emotional distress and anxiety suffered by Covered Persons as a result of their information being disclosed by Defendants.

Supporting a finding of willfulness or recklessness, the Complaints also allege that Defendants remained noncompliant for months later—far beyond the ten-business-day compliance period—with ongoing noncompliance. Such allegations are more than sufficient at the pleading stage to allege entitlement to punitive damages. *See e.g., Huggins v. FedLoan Servicing*, No. CV1921731ESCLW, 2020 WL 13645747, at *7 (D.N.J. Dec. 2, 2020) (denying motion to dismiss statutory and punitive damages under FCRA); *Tjokrowidjojo v. San Lucas*, No. CV 20-6564, 2021 WL 1143379, at *3 (E.D. Pa. Mar. 25, 2021) (noting that although plaintiff “does not use the correct language, she pleads sufficient facts to state a claim for punitive damages). The relief sought under Daniel’s Law is for that very real past, present and future harm. Defendants’ authority applying Pennsylvania law does not help them. *See* Mot. at 39. There, plaintiffs failed to allege that defendant “was even aware” of the conduct at issue, much less that it was intentional. *Boring v. Google Inc.*, 362 F. App’x 273, 283 (3d Cir. 2010).

Indeed, as this Court stated, limiting the law to where there are ‘true threats’ as Defendants’ propose, “would be analogous to closing the barn door after the horse has left.” *Atlas Data Priv. Corp. v. We Inform, LLC*, 758 F. Supp. 3d 322, 339 (D.N.J. 2024).

I. The Court Should Not Strike Plaintiffs’ Request for Injunctive Relief.

Defendants’ request to strike Plaintiffs’ request for prospective injunctive relief is both meritless and dangerous. They mount a two-fold attack, contending that (1) the Complaints allege only past injury; and (2) any injunctive relief that would be granted by the Court would somehow boil down to an impermissible “obey-the-law” injunctions. Mot. at 40–41. Neither argument holds water. Daniel’s Law empowers this Court to grant injunctive relief, which is important in these cases to protect the personal safety and privacy of these covered persons.

First, Defendants mischaracterize the injury alleged in the Complaints. Plaintiffs do not allege a single past injury with a finite ending; Plaintiffs allege repetitive and *continuing* disclosures in violation of the law. Compl. ¶ 23 (“Defendants *have not complied* with the law *by ceasing the disclosure or re-disclosure* ... of protected information”) (emphasis added). Such allegations demonstrate “a real and immediate threat” of future harm. *City of Los Angeles v. Lyons*, 461 U.S. 95, 103–04 (1983); *Snowdy v. Mercedes-Benz USA, LLC*, 2024 WL 1366446, at *9 (D.N.J. Apr. 1, 2024) (concluding allegations of “ongoing” safety risks sufficient for prospective injunctive relief and distinguishing from “stop me before I buy again” theories of injury).

Second, Plaintiffs do not intend to seek any “overbroad” injunctive relief. Plaintiffs intend to seek targeted injunctions that will have the effect of stopping the

ongoing disclosure of these covered persons’ protected information, which could take varying forms, such as barring use of data obtained from other brokers who are not in compliance or prohibiting specified disclosures, or barring disclosure of home address information such as unique assessor parcel numbers or geographic coordinates which Defendants contend is not required. Any injunction will of course give Defendants “fair notice of what conduct will risk contempt.” *Murray-Nolan v. Rubin*, No. CV 22-801 (EP) (AME), 2022 WL 4104343, at *7 (D.N.J. Sept. 8, 2022), *aff’d sub nom. Falcone v. Dickstein*, 92 F.4th 193 (3d Cir. 2024). This is unlike the injunctions at issue in the cases cited by Defendants, where plaintiffs literally requested that defendants obey the law without identifying specific acts of compliance or noncompliance. *Id.* (rejecting request to enjoin “First Amendment violations”); *Sixth Angel Shepherd Rescue Inc. v. West*, 790 F. Supp. 2d 339, 353 (E.D. Pa. 2011) (dismissing requests that defendants not “infringe upon Plaintiff’s rights” and to “enjoin behavior that would restrain officials from performing acts”), *aff’d*, 477 F. App’x 903 (3d Cir. 2012).

J. Plaintiffs’ Allegations Against Belles Camp Communications, Inc. Plausibly State a Claim for Relief.¹²

Belles Camp Communications, Inc.’s (“Belles”) Rule 12(b)(6) arguments fail because they raise factual disputes inappropriate for resolution at the pleading stage.

¹² This section addresses Defendant Belles Camp Communications, Inc.’s Supplemental Brief in Support of its Motions to Dismiss Plaintiffs’ Complaint

Belles argues that it did not possess Covered Persons’ protected information and that it is implausible for Plaintiffs to view the content of Belles’ website. But the Belles complaint specifically alleges that Belles discloses this information and includes a redacted screenshot of Belles’ website as an example of Belles’ possession of protected information. *See* Belles Compl. ¶¶ 39-40. Further, Belles willfully ignores the various means by which sophisticated internet users can access the contents of allegedly private websites, including through secondhand means.

These are merits arguments for another day. At the pleading stage, this Court is required to accept as true all factual assertions of a complaint. *Doe v. Princeton University*, 30 F. 4th 335, 342 (3d Cir. 2022). “[T]he post-*Twombly* pleading standard simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of the necessary elements.” *Connelly v. Lane Const. Corp.*, 809 F. 3d 780, 789 (3d Cir. 2016). Plaintiffs’ allegations, including a redacted screenshot of Belles’ website’s disclosure of protected information, meet these pleading requirements and raise a reasonable expectation that discovery will reveal further evidence of Belles’ violations.

(“Belles Motion”), Dkt. 49, filed in *Atlas Data Privacy Corp., et al. v. Belles Camp Communications, Inc., et al.*, No. 24-cv-04949-HB. Defendant eMerges.com Inc. submits a declaration in support of a similar fact-based argument. *See Atlas Data Privacy Corp., et al. v. eMerges.com Inc., et al.*, No. 24-cv-04434-HB, Dkt. 50-1; 50-2. For the same reasons, the eMerges.com’s arguments must be rejected.

K. Plaintiffs’ Allegations Against Innovis Plausibly State a Claim for Relief.¹³

Innovis asks the Court to treat it as a “consumer reporting agency” under the Fair Credit Reporting Act, but the question of whether Innovis qualifies as a Credit Reporting Agency under the FCRA turns on *what* Covered Persons’ information Innovis uses and *how* this information is used. *See Individual Reference Servs. Group, Inc. v. Federal Trade Comm’n*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001), *aff’d sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (“[T]he ‘credit header’ data at issue in this litigation—the name, address, social security number, and phone number of the consumer—was not subject to the FCRA.”); *Adams v. LexisNexis Risk & Info. Analytics Grp., Inc.*, 2010 WL 1931135, at *11 (D.N.J. May 12, 2010) (“‘[C]redit header’ information is not regulated by the FCRA.”). This is a factual issue that cannot be resolved at the motion to dismiss phase.

Regardless of what label is applied (data broker, people finder, reporting agency), Plaintiffs allege violations by Innovis. While there is no need to go beyond the four corners of the complaint to reject this motion, Innovis’ website—which is referenced in the Complaints—includes a page instructing visitors that they can request opting out of marketing lists that Innovis prepares and distributes to creditors

¹³ This section addresses Defendant Innovis Data Solutions, Inc.’s Memorandum of Law in Support of Innovis’s Motion to Dismiss (“Innovis Motion”), Dkt. 45-5, filed in *Atlas Data Privacy Corp., et al. v. Innovis Data Solutions, Inc., et al.*, No. 24-cv-04176-HB.

and insurers: lists that must, of necessity, include individuals' respective home addresses and unpublished phone numbers. *See* Parikh Cert. at Ex. E <https://innovis.com/personal/optOutOptIn>. The website also outlines Innovis's use of data including home address or telephone number for non-FCRA services such as receivables management and fraud prevention. *Id.* at Ex. F (<https://www.innovis.com/home/privacyNotice>). Daniel's Law's broad definition of "disclose" does not require disclosure to the general public, so Innovis's alternative argument also fails. In fact, Daniel's Law liability may attach "regardless of whether a search of such list or database is actually performed." N.J.S.A. § 58:6-166.1(d). In any case, these factual questions regarding the extent of Innovis' disclosures are not appropriate at the motion to dismiss stage. Plaintiffs allege facts establishing that Innovis discloses home address and unpublished phone numbers in violation of Daniel's Law, including through its website [Innovis.com](https://www.innovis.com). Innovis denies doing so, but like in any case, a denial of factual allegations is not a basis for dismissal.

L. Plaintiffs' Allegations Against the Zillow Defendants Plausibly State a Claim for Relief.¹⁴

The Zillow Defendants rely on the kind of fact-based arguments that courts routinely reject at the pleading stage. The Zillow Defendants contend that they do

¹⁴ This section addresses Defendants Zillow, Inc. and Zillow Group, Inc.'s ("Zillow Defendants") Motion to Dismiss Plaintiffs' Complaint ("Zillow Motion"), Dkt. 52,

not disclose or otherwise make available any covered persons’ home address or telephone number, but it is what Plaintiffs allege that matters here. Plaintiffs expressly allege that they do (*see* Zillow Compl. ¶¶ 40, 42), and the Zillow Defendants’ denial of those facts provides no basis for dismissal. These are not conclusory allegations, as suggested by the Zillow Defendants. Plaintiffs allege that the Zillow Defendants “offer and engage in the disclosure of data and information through one or more websites or applications” (*id.* ¶ 40) and that “[i]n accordance with Defendants’ business model, visitors, users, or customers may obtain” (*id.* ¶42) protected information of covered person. The Zillow Defendants’ own websites, cited in the Zillow complaint and relied upon in defendants’ motion, direct the Court to evidence that supports Plaintiffs’ factual assertions. For example, one of the Zillow Group’s Applications advertised on www.zillowgroup.com, the “Bridge Public Records API,” purports to “allows users to retrieve parcel, assessment and transactional county data” and which the Zillow Defendants advertise as a resource “for commercial use cases by businesses.”¹⁵ Such “transactional county data” includes property addresses and name of property owners, and is only one way that

filed in *Atlas Data Privacy Corp., et al. v. Zillow, Inc., et al.*, No. 24-cv-04256-HB. Citations to “Zillow Compl.” refer to the Complaint filed in that action.

¹⁵ *See* <https://www.zillowgroup.com/developers/api/public-data/public-records-api/>

the Zillow Defendants disclose or otherwise make available covered persons' protected information.

II. INNOVIS' AS-APPLIED FIRST AMENDMENT CHALLENGE FAILS.¹⁶

Innovis' First Amendment argument should be rejected for two reasons.

First, Innovis's as-applied challenge fails because there is no factual record for the Court to assess how the law is actually applied to Innovis. As applied challenges to the constitutionality of a statute are "based on a developed factual record and the application of a statute to a specific person." *Richmond Med. Ctr. for Women v. Herring*, 570 F.3d 165, 172 (4th Cir. 2009). Here, there is no factual record to assess application to Innovis. Innovis assumes both that (i) it is a credit-reporting agency under the FCRA, 15 U.S.C. § 1681a(f), and (ii) as a matter of fact, requires all customers to certify that they have a "permissible purpose" as required by the FCRA, 18 U.S.C. § 1681b(a), but neither of these facts is alleged in the Complaints, and neither of these facts is subject to judicial notice. *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir. 2007) ("private corporate websites, particularly when describing their own business" are not subject to judicial notice). Similarly, "[a] court may take judicial notice of documents filed in other court proceedings because they are matters of public record," but "cannot, however, rely on these

¹⁶ This section addresses the Innovis Motion, Dkt. 45-5, filed in *Atlas Data Privacy Corp., et al. v. Innovis Data Solutions, Inc., et al.*, No. 24-cv-04176-HB.

public records to establish facts.” *Prime Property & Cas. Ins. Inc. v. Freightway Logistics LLC*, 2019 WL 6907532, at *2 n.3 (D.N.J. Dec. 19, 2019) (citing *Lum v. Bank of Am.*, 361 F.3d 217, 221 n.3 (3d Cir. 2004)). As noted above, Innovis’s status as a Credit Reporting Agency, according to the credit industry, is dependent on *what* information Innovis uses and *how* that information is used. These factual determinations can only be resolved after conducting discovery.

Second, Innovis’ as-applied challenge fails on the merits. This Court already held that Daniel’s Law is subject to the *Florida Star* test, according to which a statute creating a privacy tort violates the First Amendment only if (i) the private information disclosed was “truthful and lawfully obtained” and concerns “a matter of public significance”; and (ii) “the imposition of liability is narrowly tailored to serve an interest of the highest order.” *Bowley v. City of Uniontown Police Dep’t*, 404 F.3d 786 n.3 (3d Cir. 2005). Innovis makes no attempt to establish that its published content constitutes speech on a matter of public concern—nor can it do so. *See* Innovis Mot. at at 23-28 (never suggesting Innovis reports are speech on a matter of public concern). As this Court has already held, “home addresses and unpublished phone numbers are not matters of public significance.” *We Inform, LLC*, 758 F. Supp. 3d 322 at 339 .

Nor can Innovis establish that imposing liability on it is not “narrowly tailored to serve an interest of the highest order.” *Bowley*, 404 F.3d at 786. Innovis concedes

that Daniel’s Law serves “privacy” and “safety” interest of the highest order. Innovis Mot. at 27. But Innovis claims—absurdly—that Daniel’s Law will “often serve to prevent, or obstruct, a covered person’s own attempts to seek credit” and can “block or otherwise restrict *a transaction requested by the consumer.*” This ignores that Daniel’s Law only gives rise to a nondisclosure duty 10 days after a covered person submits a written nondisclosure request. N.J.S.A. § 56.8-166.1a(1). Unless a consumer-reporting agency has received a nondisclosure request from a covered person, providing a report in a transaction requested by that person would not give rise to liability under the statute. And if a covered person *has* submitted a nondisclosure request, the consumer-reporting agency has notice that consent from that covered person is necessary to disclose their contact information in a credit report and can request the covered person’s consent before disclosing their address or phone number a report.

Moreover, Innovis can simply redact addresses and phone numbers from reports because addresses and phone numbers are credit-header information, which is not regulated by the FCRA. *See* 15 U.S.C. § 1681c(d); *Individual Reference Servs. Group, Inc. v. Federal Trade Comm’n*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001), *aff’d sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (“[T]he ‘credit header’ data at issue in this litigation—the name, address, social security number, and phone number of the consumer—was not subject to the FCRA.”); *Adams v.*

LexisNexis Risk & Info. Analytics Grp., Inc., 2010 WL 1931135, at *11 (D.N.J. May 12, 2010) (“‘[C]redit header’ information is not regulated by the FCRA.”).¹⁷

III. EXTRATERRITORIALITY DOES NOT BAR PLAINTIFFS’ CLAIMS AGAINST DEFENDANTS.¹⁸

Defendants We Inform, Infomatics, The People Searchers and eMerges.com claim that Daniel’s Law does not apply to them under the doctrine of extraterritoriality businesses and associations fails as a matter of law and fact. Defendants’ sweeping argument that Plaintiffs’ “claims are based on conduct outside New Jersey” (Mot. at 14) is contradicted by the factual allegations, where Plaintiffs detail how Defendants disclosed home addresses and telephone numbers of New Jersey residents for commercial gain, even after thousands of New Jersey residents covered by Daniel’s Law instructed them to stop. This request for dismissal also

¹⁷ Innovis asserts that—despite this Court’s prior ruling—this challenge is governed by intermediate scrutiny rather than the *Florida Star* test because its reports constitute commercial speech. Doc. 45-4 at 23-24 & n.8. Regardless Daniel’s Law clearly exhibits a “proportionate fit between its substantial interest and [the] legislative attempt to advance that interest” for the same reason the statute is narrowly tailored under *Florida Star*. *Greater Philadelphia Chamber of Commerce v. City of Philadelphia*, 949 F.3d 116, 156 (3d Cir. 2020) (even an “overbroad” statute with a reasonable degree of fit satisfies “intermediate scrutiny”).

¹⁸ This section addresses Defendants We Inform, LLC (“WeInform”), Infomatics, LLC (“Infomatics”), The People Searchers, LLC (“People Searchers”) Supporting Brief in Support of Their Motions to Dismiss the Complaints (“*Infomatics* Motion”), Dkt. 46-1, filed in *Atlas Data Privacy Corp., et al. v. Infomatics, LLC, et al.*, No. 24-cv-04041-HB. Defendant eMerges.com Inc. also joins the *Infomatics* Motion. See *Atlas Data Privacy Corp., et al. v. eMerges.com Inc., et al.*, No. 24-cv-04434-HB, Dkt. 50-1; 50-2. Citations to “Mot.” in this section refer to the *Infomatics* Motion.

ignores applicable New Jersey statutory interpretation principles on extraterritoriality and the distinct purpose of Daniel’s Law, which is to protect the privacy and security rights of New Jersey citizens.

There is no presumption that New Jersey statutes only apply to defendants that reside within the state’s borders. *See Turner v. Aldens, Inc.*, 179 N.J. Super. 596, 605 (App. Div. 1981) (rejecting “a presumption that because the act contains no express words of extraterritorial application, the foreign retail seller is insulated from operation of that law”). New Jersey courts determine applicability of New Jersey statutes to out-of-state defendants using normal statutory interpretation principles. *See Schulman v. Zoetis, Inc.*, 684 F. Supp. 3d 275 (D.N.J. 2023); *Real v. Radir Wheels, Inc.*, 198 N.J. 511, 524 (2009). Where the statutory definitions provide no state-based limitations, no territorial limits apply. *Calabotta v. Phibro Animal Health Corp.*, 460 N.J. Super. 38, 61 (2019); *Turner*, 179 N.J. Super. at 602.

Here, Daniel’s Law does not limit its application to businesses or associations with operations or sales in New Jersey. Daniel’s Law broadly prohibits the disclosure of protected information without any mention of a geographic limitation and the “person, business or association” subject to the law are not defined as limited to New Jersey residents. *See* N.J.S.A. § 56:8-166.1(a).¹⁹ Given the absence of any

¹⁹ Conversely, the New Jersey Legislature knows how to limit statutes to in-state actors when it wants to and has explicitly included geographic limitations in definitions for other laws to this effect. *See, e.g.*, N.J.S.A. § 56:8-166.4 (defining

territorial limits in the statute itself, there is no basis for dismissal based on any extritoriality.

Rejecting this argument is also consistent with the purposes of Daniel’s Law. *See, e.g., Mehlman v. Mobil Oil Corp.*, 153 N.J. 163, 195-96 (1998) (declining “to impose artificial geographical limits” based on “the purposes” of a New Jersey whistleblower statute). Courts have repeatedly held that consumer protection and privacy statutes intended to protect New Jerseyans apply to out-of-state and in-state defendants alike. *See Oxford Consumer Discount Co. of North Philadelphia v. Stefanelli*, 102 N.J. Super. 549, 565 (1968) (applying the New Jersey Secondary Mortgage Loan Act to out-of-state defendant because “the manifest purpose” of enacting the statute was “to protect New Jersey residents from overreaching mistreatment of them by out-of-state as well as local lenders”); *State v. Worthy*, 141 N.J. 368, 379 (1995) (“[T]here can be no doubt that the legislative concern for privacy embraces the privacy interest that a resident in New Jersey has in telephone conversations that originate from an out-of-state telephone.”); *Turner*, 179 N.J. Super. at 602 (holding that the “evil sought to be remedied” by a New Jersey consumer protection statute necessitated protection “from that evil irrespective of whether its source was in-state or out-of-state”).

“Consumer” as “an identified person *who is a resident of this State* acting only in an individual or household context”).

The purpose of Daniel’s Law is in-line with these consumer and privacy laws, seeking to protect New Jersey residents regardless of state boundaries. Daniel’s Law is intended “to enhance the safety and security of certain public officials in the justice system,” N.J.S.A. § 56:8-166.3, which is a compelling “government interest of the highest order.” *Kratovil v. City of New Brunswick*, No. A-0216-23, 2024 WL 1826867 at *4 (N.J. App. Div. Apr. 26, 2024).

This purpose “of the highest order” would be directly frustrated if out-of-state businesses and associations could simply continue to disclose the personal information of Covered Persons on the internet after receiving nondisclosure requests. Businesses and associations operate nationwide, and the protected information they disclose on the internet is available around the country, including in New Jersey. Limiting the geographic scope of Daniel’s Law to in-state companies when those companies are acting within New Jersey’s borders (or otherwise satisfying the requirements for personal jurisdiction) would undermine the protections afforded by Daniel’s law, and that cannot be the proper interpretation of Daniel’s law. Indeed, such a limitation would not have prevented the murder that was the genesis for the law’s creation and run contrary to the Legislature’s direction that the law be liberally construed to “accomplish its purpose . . . to enhance the safety and security of” covered persons. N.J.S.A. 56:8-166.3.

The lack of merit to this argument²⁰ is only further demonstrated by the cases cited by these defendants. Most of those cases involved a distinct legal question limited to a specific employment law context. *See Peikin v. Kimmel & Silverman, P.C.*, 576 F. Supp. 2d 654 (D.N.J. 2008); *D’Agostino v. Johnson & Johnson, Inc.*, 133 N.J. 516, 628 A.2d 305 (1993); *Abrams v. eResearch Tech., Inc.*, 703 F. Supp. 3d 593 (E.D. Pa. 2023). Defendant points to no instance in which a statute similar to Daniel’s Law was limited to in-state defendants. The cases cited by these defendants are also factually distinguishable in that they did not involve conduct directed at New Jersey residents that threatens the privacy and safety of those New Jersey residents. In fact, for those cases that involved such conduct, the Court found that there *was* jurisdiction. *Compare McDonnell v. State of Ill.*, 163 N.J. 298, 301-

²⁰ Defendants’ argument regarding extraterritoriality and ‘conduct on the Internet’ is similarly meritless. Mot. at 15. This is because the mere extraterritorial reach of the internet does not limit a statute related to online conduct to defendants residing in a specific state. As noted in the cases Defendants cite, application of dormant commerce clause is relevant to such an analysis. *See, e.g., American Libraries Ass’n v. Pataki*, 969 F. Supp. 160, 168-69 (S.D.N.Y. 1997). While extraterritorial application of a statute may violate the Commerce Clause where it would result in “inconsistent legislation” from other states, Daniel’s Law relates to whether businesses and associations can disclose the information of New Jersey public servants and therefore has no risk of inconsistent legislation from other States. *See Instructional Sys., Inc. v. Computer Curriculum Corp.*, 35 F.3d 813, 826 (3d Cir. 1994); *cf. In re Insulin Pricing Litig.*, No. 2:17-CV-00699 (BRM) (RLS), 2024 WL 5252471 (D.N.J. Dec. 31, 2024) (“Defendants do not explain how uniformly applying consumer protection statutes to all manufacturers, regardless of location, is designed to benefit in-state economic interests by burdening out-of-state competitors.”) (internal quotation marks omitted).

02 (N.J. 2000) (applying New Jersey age discrimination law to defendant State of Illinois where New Jersey resident worked in Illinois Department of Revenue’s New Jersey field office), *with D’Agostino*, 133 N.J. at 539-40 (“New Jersey law regulates conduct in New Jersey, such as J & J’s alleged orchestration of the bribing of a foreign official and firing of plaintiff.”). For these reasons, Defendants’ extraterritoriality arguments fail and the motion should be denied.

IV. DEFENDANT INNOVIS’ PREEMPTION ARGUMENTS ARE MERITLESS AND BARRED.²¹

Dismissal under Federal Rule of Civil Procedure 12(b)(6) is not appropriate unless “preemption is manifest in the complaint itself.” Lexis Order at 16.²² (citing *Lupian v. Joseph Cory Holdings LLC*, 905 F.3d 127, 130-31 (3d Cir. 2018) (affirming denial of dismissal sought based on preemption)). There is no preemption by the Fair Credit Reporting Act (“FCRA”), and certainly no “manifest” preemption as the FCRA does not preempt Daniel’s Law. Indeed, as both the credit reporting industry has argued over almost two decades, and as the regulators have held, the information at issue—home addresses and unpublished home telephone numbers—is not part of a credit report.

²¹ This section addresses the Innovis Motion, Dkt. 45-5, filed in *Atlas Data Privacy Corp., et al. v. Innovis Data Solutions, Inc., et al.*, No. 24-cv-04176-HB.

²² *John Doe-1 et al. v. LexisNexis Risk Solutions, Inc.*, Case No. 1:24-cv-04566-HB, Dkt. 66 (“Lexis Order”).

A. Whether Innovis Is Acting as a CRA is a Factual Issue.

Innovis claims that it is acting as a “consumer reporting agency (CRA)” in these cases, but that is a factual issue not proper for a motion to dismiss. *Red Hawk Fire & Sec., LLC v. Siemens Indus. Inc.*, 449 F. Supp. 3d 449, 469 (D.N.J. 2020) (“It is inappropriate for the Court to wade into factual issues. . . on a motion to dismiss.” (citation omitted)). In fact, Plaintiffs have alleged in these actions that various purported “consumer reporting agencies (CRA)”-defendants have been selling consumer information for purposes that have nothing to do with their consumer credit reporting products. Plaintiffs alleged that both Innovis and LexisNexis, for example, have been disclosing or re-disclosing covered persons’ home addresses and phone numbers on the Internet and that their business models allow visitors, users, or customers to obtain this information from their websites, which has nothing to do with consumer reporting. Innovis Compl. ¶¶ 37–40. Innovis’ assumes too much at the pleading stage. Its entire argument relies on assumption that the Complaint alleges that it is acting as a CRA, but Plaintiffs have made no such allegation. Thus, there is no legal basis for Innovis to make its preemption argument.

B. Daniel’s Law is Not Preempted by the FCRA.

FCRA preempts “some but not all actions brought pursuant to state laws.” Lexis Order at 16. Under 15 U.S.C. § 1681t(a), Congress provided that state statutes “addressing the collection, distribution, or use of any information on consumers”

may “coexist with the FCRA except to the extent that those laws are inconsistent with any provision of [the FCRA].” This express preservation of statute state authority reflects Congress’s intent to allow “more protective” consumer-reporting statutes and to give states the ability to address “emerging problems affecting their local economies and citizens.” *The Fair Credit Reporting Act’s Limited Preemption of State Laws*, 87 Fed. Reg. 41,042 (Jul. 11, 2022); *Consumer Data Indus. Ass’n v. Platkin*, 2024 WL 1299256, at *6 (D.N.J. Mar. 27, 2024).

The information under Daniel’s Law (addresses and home phone numbers) is considered credit header information that is not regulated by the FCRA at all. 15 U.S.C. § 1681c(d). Definitive FTC guidance also says credit header data is not regulated by the FCRA. *Individual Reference Servs. Group, Inc. v. Federal Trade Comm’n*, 145 F. Supp. 2d 6, 17 (D.D.C. 2001), *aff’d sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002) (“In 2000, the FTC stated that the ‘credit header’ data at issue in this litigation—the name, address, social security number, and phone number of the consumer—was not subject to the FCRA because it ‘does not bear on creditworthiness, credit capacity, credit standing, character, general reputation, personal characteristics, or mode of living, unless such terms are given an impermissibly broad meaning.’”).

And that is exactly what the credit reporting industry has argued for almost two decades. *See e.g., Individual Reference Servs. Group, Inc. v. Federal Trade*

Comm’n, 145 F. Supp. 2d 6 at 17, *aff’d sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (“[T]he ‘credit header’ data at issue in this litigation—the name, address, social security number, and phone number of the consumer—was not subject to the FCRA.”); *Adams v. LexisNexis Risk & Info. Analytics Grp., Inc.*, 2010 WL 1931135 at *11. In addition to Innovis, that is what defendant LexisNexis also argued to this Court a few years ago in *Adams*, at *11 (“Lexis also notes in its brief that information obtained from consumer reporting agencies constituting ‘credit header’ information is not regulated by the FCRA.”). Until the advent of Daniel’s Law, Innovis (and LexisNexis) can point to no other FCRA case where it (or another similarly situated defendant) has argued that address and telephone information are part of the FCRA-consumer report. Defendants cannot have their cake and eat it too, treating information as of one kind to make money one way, only to take a completely inconsistent position elsewhere to keep profits there as well.

Innovis relies on § 1681t(b)(1)(E), which bars state laws regulating “any subject matter regulated under... section 1681c... relating to information contained in consumer reports.” Innovis Mot. at 20. Section 1681c provides that information about bankruptcies that are over 10 years old and other debts that are over 7 years old cannot be in a credit report. That has no application here, and that in no way preempts Daniel’s Law. Section 1681t(b)(1)(E) preempts only those laws that regulate the *same subject matter* as § 1681c—namely, the age and type of adverse

information in reports. 26 F.4th at 7; *see also Platkin* at *10. “[E]ven when there is an express preemption clause, a court will diligently determine the substance and scope of Congress’ displacement of state law.” *Calabria Ristorante, Inc. v. Ruggiero Seafood, Inc.*, 2023 WL 8643781 at *8 (D.N.J. Dec. 14, 2023).

Daniel’s Law does not impose restrictions on those categories, as it only deals with information outside of consumer credit reports. Innovis is not required to include addresses and home phone numbers in its consumer reports. It can easily issue credit reports without the optional header information, or it can easily redact that information from the reports. Addresses and phone numbers are the “kind of information [that] appears on a credit report,” ***not information that is required to be in one.***²³ There is no conflict with Daniel’s Law.

Innovis’ reliance on *Pladeck v. Credit Suisse First Fin. Corp.*, 2024 WL 4601461 (D.N.J. Oct. 29, 2024) is misplaced. *See* Innovis Mot. at 18. In *Pladeck*, the court applied total preemption to bar state-law claims against furnishers of information to CRAs—conduct expressly governed by the FCRA’s accuracy provisions. That case did not involve the disclosure of protected information or

²³ *What Is a Credit Report?* Consumer Fin. Prot. Bureau, <https://www.consumerfinance.gov/ask-cfpb/what-is-a-credit-report-en-309/> (Jan. 29, 2024); Credit Reports and Credit Scores, Bd. of Governors of the Fed. Rsrv. Sys., https://www.federalreserve.gov/creditreports/pdf/credit_reports_scores_2.pdf (last visited April 18, 2025).

consider the type of law at issue here. As the *Pladeck* court emphasized, the FCRA was enacted “to protect consumers from the transmission of inaccurate information about them, and to establish credit reporting practices that utilize accurate, relevant, and current information in a confidential and responsible manner.” *Id.* at 3 (*quoting Seamans v. Temple Univ.*, 744 F.3d 853, 860 (3d Cir. 2014)). Daniel’s Law has nothing to do with the disclosure of “inaccurate information.” Indeed, it is the disclosure by Innovis and others of **accurate** information that puts covered persons in danger. It is inherently improbable that Daniel’s Law would be in any way inconsistent with the FCRA, nor do Plaintiffs seek to assert claims in this action that in any way undermine or conflict with application of the FCRA. Innovis does not point to a single section of the FCRA establishing that addresses and phone numbers—the sole information at issue here—must be part of a “consumer report”.

Finally, Innovis argues that because Daniel’s Law adds to the list of data excluded under § 1681c, it is therefore, preempted. But this again assumes that address and telephone numbers are part of consumer reports, which defendants have long conceded that they are not. Regardless, it misstates the nature of the statute and the FCRA’s preemption framework. Daniel’s Law is consistent with the well-established principle that states may adopt “more protective” rules. *The Fair Credit Reporting Act’s Limited Preemption of State Laws*, 87 Fed. Reg. 41,042 (Jul. 11, 2022). As such, Innovis’s suggestion that state laws such as Daniel’s Law are

somehow incompatible with the FCRA cannot be reconciled with the statute's text, purpose, or judicial interpretation.

C. Daniel's Law Does Not Interfere with FCRA's Opt-Out System.

Innovis' assertion that Daniel's Law is also preempted by 15 U.S.C. § 1681b, based on its purported interference with the FCRA's opt-out framework, is similarly unfounded. *See* Innovis Mot. at 22. Daniel's Law operates in a wholly different context: it concerns disclosures of personal contact information, not the internal operation of prescreening systems or the conditions under which a consumer reporting agency may provide a consumer report for a firm offer of credit. Plaintiffs' nondisclosure requests are in no way inconsistent with § 1681b(2)(A) and (C) – they are consistent with it, seeking to prevent disclosure of this information.

Daniel's Law is not an opt-out from prescreened credit offers. It is a public safety and privacy statute that prohibits disclosure, re-disclosure, or otherwise making available certain protected information after the individual has submitted a nondisclosure request. Plaintiffs do not seek to restrict the furnishing of consumer reports to creditors or insurers, nor do they seek to alter how prescreening operates. They only seek to protect the privacy and safety of covered persons by preventing disclosure of specific information. The FCRA does not regulate public disclosures of information outside of the consumer report context, and nothing in § 1681b prohibits states from enacting privacy laws that address such conduct.

Even if the FCRA’s opt-out provisions were implicated here—which they are not—Plaintiffs’ nondisclosure requests are functionally aligned with the consumer rights the FCRA already recognizes. Section 1681b allows consumers to exclude their name and address from prescreened lists; Daniel’s Law allows designated covered persons to prevent their home addresses and phone numbers from being disclosed. In both cases, the purpose is to give consumers control over their own data. Where federal and state laws serve complementary purposes, preemption does not apply. *See Consumer Data Indus. Ass’n v. Frey*, 26 F.4th 1 at 6 (1st Cir. 2022); *Platkin*, 2024 WL 1299256, at *10.²⁴

FCRA’s text and structure confirm that Congress did not intend to occupy the entire regulatory field of consumer data, and instead meant to complement it. *Consumer Data Indus. Ass’n v. Frey*, 26 F.4th 1, 6 (1st Cir. 2022) (§1681t does not preempt all state laws “relating to information contained in consumer reports.”); *Galper v. JPMorgan Chase Bank, N.A.*, 802 F.3d 437, 447 (2d Cir. 2015) (“The FCRA plainly does not preempt the entire field.”); *Davenport v. Farmers Ins. Grp.*, 378 F.3d 839, 845 (8th Cir. 2004) (similar). Indeed, the text of § 1681t(a) confirms that the FCRA “does not annul, alter, affect, or exempt any person... from

²⁴ Critically, if Innovis truly believed the FCRA’s opt-out mechanism governed the disclosure of names and addresses, it should have honored Plaintiffs’ nondisclosure requests—whether under Daniel’s Law or under the FCRA itself.

complying with the laws of any State... except to the extent that those laws are inconsistent.”

Finally, Innovis fails to point to any provision of the FCRA that affirmatively requires consumer reporting agencies to publish home addresses or phone numbers online or to furnish them without regard to opt-out requests. As with its argument under § 1681c, Innovis seeks to convert the FCRA into a mandate that eliminates state privacy rights, despite the FCRA’s express language preserving state laws that are not inconsistent with federal provisions. *See* 15 U.S.C. § 1681t(a).

V. DEFENDANTS CANNOT INVOKE IMMUNITY UNDER SECTION 230 OF THE COMMUNICATIONS DECENCY ACT.²⁵

Like extraterritoriality, immunity under the Communications Decency Act (“CDA”), 47 U.S.C. § 230 (“Section 230”) is an argument that only some defendants present: Defendants Smarty, WeInform, Infomatics and The People Searchers argue that they are immune from Plaintiffs’ claims under Section 230. This request for dismissal also fails for multiple reasons.

²⁵ This section addresses the *Infomatics* Motion, Dkt. 46-1, filed in *Atlas Data Privacy Corp., et al. v. Infomatics, LLC, et al.*, No. 24-cv-04041-HB, and Defendants Smarty, LLC and SmartyStreets, LLC’s (“Smarty”) Memorandum of Law in Support of Their Motion to Dismiss (“Smarty Mot.”), Dkt. 34-1, filed in *Atlas Data Privacy Corp., et al. v. Smarty, LLC, et al.*, No. 24-cv-08075-HB.

A. CDA Immunity is Not Established from Plaintiffs’ Complaints.

Dismissal on the basis of an affirmative defense like Section 230 is only appropriate “if the predicate establishing the defense is apparent *from the face of the complaint*.” *Brody v. Hankin*, 145 F. App’x 768, 771 (3d Cir. 2005). Defendants have the burden of satisfying the elements of Section 230 based on the allegations in the Complaints—which they have failed to do. Nothing in the Complaints establish that Defendants are “treated as the publisher or speaker of any information provided by another information content provider,” and, importantly, Plaintiffs “need not affirmatively negate *any* of the elements of Section 230.” *Moretti v. Hertz Corp.*, No. CV 14-469-LPS, 2017 WL 1032783, at *3 (D. Del. Mar. 17, 2017); *see e.g., Krause, v. RocketReach, LLC*, 561 F. Supp. 3d 778 (N.D. Ill. Sept. 21, 2021) (rejecting CDA immunity argument where complaint allegations did not establish Section 230 elements).

Instead, Defendants rely on extraneous evidence from Defendants’ websites (including Defendants’ online privacy policy not cited in the Complaints) and ask this Court to discern complex factual questions—like whether Defendants obtain covered person’s information from another publisher, and what editorial functions Defendants perform. *Infomatics* Mot. at 20. These factual inquiries, including the veracity of the statements on Defendants’ websites, are clearly beyond the scope of a motion to dismiss. *See Victaulic Co.*, 499 F.3d 227, 236 (“private corporate

websites, particularly when describing their own business” are not subject to judicial notice). There are no alleged facts in the Complaints that support the Defendants’ claim for immunity, thus, the inquiry ends here.

The same Section 230 argument advanced by Defendants here has been rejected by at least one New Jersey state court as premature. *See* Parikh Cert. at Ex. G, Transcript of Hearing on Motion to Dismiss in *Atlas, et al. v. Twilio, Inc., et al.*, MRS-L-000226-24, at 49:15-20 (“[W]hether or not Twilio itself is just information that it’s getting from somebody else, whether it’s creating some type of content by matching a variety of sources, whether it is performing some kind of editing function, whether it adds information to its system, all of that information is well beyond the scope of the -- the complaint.”); *id.* 49:24-25 (“it is simply just too premature for the Court...to consider that application [of Section 230].”). This Court should likewise reject Defendants’ bid to find Section 230 immunity.

B. Defendants Cannot Satisfy the Requirements for Section 230 Immunity.

Even if the CDA applies to Daniel’s Law claims (it does not),²⁶ Defendants’ motion should be denied because they have not satisfied and cannot satisfy the second and third prongs of Section 230 immunity.

²⁶ Section 230 immunity does not apply to laws *pertaining* to intellectual property, as courts have broadly defined that term. *See Hepp v. Facebook*, 14 F.4th 204, 205 (3d Cir. 2021) (finding state laws “pertaining to” the subject of intellectual property are exempt from Section 230 immunity). Daniel’s Law is a state privacy law that

Under the second prong, a plaintiff’s claim must require that the defendant be “treated as the publisher or speaker of information.” 47 U.S.C. § 230(c)(1). “[W]hat matters is not the name of the cause of action, but rather whether the cause of action inherently requires the court to treat the defendant as the ‘publisher or speaker’ of content provided by another.” *Def. Distributed v. Platkin*, 697 F. Supp. 3d 241, 273 (D.N.J. 2023) (quoting *Backpage.com, LLC v. Hoffman*, No. 13-03952, 2013 WL 4502097, at *6 (D.N.J. Aug. 20, 2013)). A plaintiff’s claim only treats the defendant as the publisher or speaker of any information if it (1) “makes the defendant liable for publishing certain information to third parties, and (2) seeks to impose liability based on the information’s improper content.” *Henderson v. Source for Pub. Data, L.P.*, 53 F.4th 110, 120–21 (4th Cir. 2022). Liability under Daniel’s Law meets neither of these requirements.

First, nothing in Daniel’s Law requires the Covered Persons’ information be published to third parties for liability to attach. The statute expressly provides for liability “regardless of whether a search of such list or database is actually performed.” N.J.S.A. 56:8-166.1(d)(3) (emphasis added). Liability under Daniel’s Law is triggered only when a defendant fails to comply with a covered person’s

also protects a covered person’s intellectual property rights one holds in their name and protected information. *See Vidal v. Elster*, 602 U.S. 286, 301–07 (2024) (tracing the history of and linking common law privacy rights to intellectual property). Defendants cannot, therefore, invoke Section 230 immunity.

written request for nondisclosure after ten business days. *Id.* at 56:8-166.1(a)(1). If a defendant complies with a covered person’s request within the statutory period, it is not liable under Daniel’s Law. For a defendant to fit within Section 230, the focus of its liability must be on the content of the information as opposed to, like here under Daniel’s Law, its own actions. *See e.g., Erie Ins. Co. v. Amazon.com, Inc.*, 925 F.3d 135, 139 (4th Cir. 2019) (rejecting Section 230 immunity because the plaintiff’s product-liability claim was premised on Amazon’s conduct of selling a defective product, not Amazon’s publication of the product on its website); *F.T.C. v. Accusearch Inc.*, 570 F.3d 1187, 1204–05 (10th Cir. 2009) (Tymkovitch, J., concurring) (rejecting Section 230 immunity where “the FTC sought and ultimately held [defendant] liable for its *conduct* rather than for the *content* of the information it was offering on [its] website”).

Second, liability under Daniel’s Law is not based on any “improper content” of published speech. *Henderson*, 53 F.4th 110 at 122 (“[F]or § 230(c)(1) protection to apply, we require that liability attach to the defendant on account of some improper content within their publication.”). Here, there is no question that the published content—home addresses and unpublished home telephone numbers—is true and accurate. That’s the point—publishing this accurate information puts covered persons at risk. Because there is nothing inherently wrong about the content itself, the “improper-content requirement” articulated in *Henderson* for Section 230

immunity to apply is not met. Indeed, Daniel’s Law is ‘agnostic’ about the substantive content or message expressed by the speaker, and there is no allegation that this information was untruthful or that Defendants obtained it illegally.²⁷ Defendants’ liability is, therefore, not based on the unlawfulness of the speech itself; liability is based on Defendant’s own noncompliance with the nondisclosure requests. Daniel’s Law does not seek to hold Defendant liable for its conduct as a “publisher or speaker,” and Section 230 immunity does not apply.

The third prong asks whether Defendants’ material was provided by “another information content provider.” 47 U.S.C. § 230(c)(1). Courts in the Third Circuit focus this analysis on whether the defendant materially contributed to the published pieces of information relevant to liability. *See, e.g., Pace v. Baker-White*, 432 F. Supp. 3d 495, 508 (E.D. Pa. 2020), *aff’d*, 850 F. App’x 827 (3d Cir. 2021). Section 230 immunity only extends to a publisher’s “traditional editorial functions - such as deciding whether to publish, withdraw, postpone, or alter content” originating from an entity other than itself. *Def. Distributed*, 697 F. Supp. 3d 241 at 274. But if a Defendant plays a role in generating the content—*e.g.*, by “solicit[ing] requests” for information and then transforming it into “a publicly available commodity”—there

²⁷ Plaintiffs’ Daniel’s Law claim is distinguishable from those Section 230 cases in which a plaintiff seeks to hold the defendant liable for the improper content posted on its website. *C.f. Green v. America Online*, 318 F.3d 465 (3d Cir. 2003) (granting § 230 immunity where claim against AOL was based on defamatory and harmful content posted in chatroom).

is no immunity because Defendants’ conduct extends beyond traditional editorial functions. *Accusearch Inc.*, 570 F.3d 1187 at 1198–1201.

Defendants are not exercising mere editorial functions here. As alleged, Defendants take an active role in soliciting and obtaining specifically sought Covered Persons’ information, including unpublished content, and curating it for publication to its customers. Compl. ¶¶ 33–34; *see e.g., Anderson v. TikTok, Inc.*, 116 F.4th 180, 184 (3d Cir. 2024) (holding Section 230 does not apply when defendants “curate compilations” of others’ content via their expressive algorithms); *Lukis v. Whitepages Inc.*, 454 F. Supp. 3d 746, 763 (N.D. Ill. 2020) (declining to dismiss IRPA claim against defendant “alleged to have actively compiled and collated, from several sources, information regarding” the plaintiff); *Kellman v. Spokeo, Inc.*, 599 F. Supp. 3d 877, 898 (N.D. Cal. 2022) (finding no immunity where defendant actively took content from other sources, curated it, and uploaded it to its site); *Pace*, 432 F. Supp. 3d 495 at 508 (finding no immunity where defendant’s website was not a “typical Internet bulletin board[,]” and finding it was “much more than a passive transmitter”).²⁸ Thus, the Complaints plausibly allege that the

²⁸ Although Plaintiffs maintain that the Court should not look beyond the Complaint, WeInform, Infomatics and The People Searchers’ websites facially refute Defendants’ Section 230 argument: “Services are owned and operated by [defendant] and contain material which is ***derived in whole or in part from material supplied by [defendant]*** and its partners, as well as other sources, . . . The Services are also protected as a ***collective work or compilation***... ***You acknowledge that the Services have been developed, compiled, prepared, revised, selected, and arranged***

“essential published content” at issue in this case was not merely acquired from another content information provider, and Defendants cannot meet Section 230’s immunity requirements.

VI. PLAINTIFFS SHOULD HAVE THE OPPORTUNITY TO CORRECT ANY DEFICIENCIES.

Plaintiffs have stated facts to sufficiently plead every element of a Daniel’s Law violation against Defendants. That said, should this Court find any deficiency exist, the interests of justice demand that leave to amend be freely granted. *Foman v. Davis*, 371 U.S. 178, 182 (1962). Therefore, any ruling in favor of Defendants should be without prejudice so that Plaintiffs have an opportunity to cure any deficiencies by amendment.

CONCLUSION

For these reasons, Plaintiffs respectfully request that this Court deny Defendants’ Consolidated Motion to Dismiss in its entirety.

Respectfully submitted,

By: /s/ Rajiv D. Parikh
Rajiv D. Parikh

by [defendant].” See Parikh Cert. at Exs. H-J. Similarly, Smarty’s website confirms it “aggregates” data so that users can access them in bulk for a “holistic” view. See Parikh Cert. at Ex. K. Such customization clearly goes beyond a mere editorial function and takes Defendants out of the scope of CDA’s immunity.